UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KELLY MONASTIRIAKOS, individually and on behalf of all others similarly situated, Plaintiff, v. ABBOTT LABORATORIES EMPLOYEES CREDIT UNION d/b/a ALEC, Defendant.	Case No. 1:24-cv-11823 **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Kelly Monastiriakos ("Plaintiff") individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against Abbott Laboratories Employees Credit Union d/b/a ALEC ("Defendant"). Plaintiff alleges the following upon information and belief based on and upon the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII") that was impacted in a data breach that Defendant publicly disclosed in October 2024 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard PII that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a credit union headquartered in Gurnee, Illinois.[1]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On or about September 23, 2024, Defendant became aware of a security incident on its IT Network.[2] Upon discovering the incident, Defendant launched an investigation with the help of leading cyber security experts to determine the nature and scope of the incident.[3] As a result of the investigation, Defendant determined that an unauthorized third-party gained access to its IT Network on August 2, 2024.[4]

6. Defendant launched a comprehensive review of the incident to determine whether sensitive information was compromised and how many individuals were impacted.[5] On September 23, 2024, the review was completed, and Defendant confirmed that sensitive personal information was indeed impacted.[6] On October 18, 2024, Defendant issued a public disclosure about the data breach and started sending notice letters to individuals impacted.[7]

7. Upon information and belief, the following types of PII was compromised as a result of the Data Breach: name, Social Security number, and financial account information.[8]

8. Defendant failed to take precautions designed to keep individuals' PII secure.

---

[1] *See About ALEC, ALEC*, https://www.alecu.org/membership/membership-benefits/about-alec (last visited Nov. 14, 2024).
[2] *Data Breach Notifications: Abbott Laboratories Employees Credit Union ("ALEC")*, OFFICE OF THE ATTORNEY GENERAL OF MAINE (October 18, 2024), https://www.maine.gov/cgi-bin/agviewerad/ret?loc=1394 (last visited November 14, 2024).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*

9. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the PII collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the PII, yet breached its duty by failing to implement or maintain adequate security practices.

10. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

11. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their PII and are subject to an increased risk of identity theft.

12. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' PII.

13. As a result of Defendant's inadequate digital security and notice process, Plaintiff and Class Members' PII was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their PII; the loss or diminished value of PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

14. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class

Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

15. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence, negligence *per se*, breach of implied contract, and unjust enrichment.

16. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

17. Plaintiff Kelly Monastiriakos is a resident of Lake Zurich, Illinois. On October 18, 2024, Defendant sent Plaintiff a notice letter informing her that her PII was impacted in the Data Breach. As a result of the Data Breach, Plaintiff has experienced an uptick in spam calls, texts, and emails. Furthermore, Plaintiff has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm.

Defendant

18. Defendant is an Illinois nonprofit corporation with its headquarters and principal place of business at 325 Tri-State Parkway, Gurnee, Illinois 60031.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members.

20. This Court has personal jurisdiction over Defendant because Defendant is registered to do business, and maintains its principal place of business, in Gurnee, Illinois.

21. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in this District, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and Plaintiff resides in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

22. Defendant is a credit union serving Abbott and AbbVie companies' current and former employees and their relatives. According to its website, Defendant provides services to "more than 31,000 individuals around the country."[9]

23. Upon information and belief, Defendant made promises and representations to individuals, including Plaintiff and Class Members, that the PII collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[10]

24. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the PII of Plaintiff and Class Members,

[9] *See About ALEC*, ALEC, https://www.alecu.org/membership/membership-benefits/about-alec (last visited Nov. 14, 2024).
[10] *Privacy Policy*, ALEC, https://www.alecu.org/membership/about/privacy-policy (last visited Nov. 14, 2024).

Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' PII from disclosure to third parties.

B. The Data Breach

26. On or about September 23, 2024, Defendant became aware of a security incident on its IT Network.[11] Upon discovering the incident, Defendant launched an investigation with the help of leading cyber security experts to determine the nature and scope of the incident.[12] As a result of the investigation, Defendant determined that an unauthorized third-party gained access to its IT Network on August 2, 2024.[13]

27. Defendant launched a comprehensive review of the incident to determine whether sensitive information was compromised and how many individuals were impacted.[14] On September 23, 2024, the review was completed, and Defendant confirmed that sensitive personal information was indeed impacted.[15] On October 18, 2024, Defendant issued a public disclosure about the Data Breach and started sending notice letters to individuals impacted.[16]

28. Upon information and belief, the following types of PII was compromised as a result of the Data Breach: name, Social Security number, and financial account information.[17]

29. Plaintiff's claims arise from Defendant's failure to safeguard her PII and failure to provide timely notice of the Data Breach.

30. Defendant failed to take precautions designed to keep individuals' PII secure.

---

[11] *Data Breach Notifications: Abbott Laboratories Employees Credit Union ("ALEC")*, OFFICE OF THE ATTORNEY GENERAL OF MAINE (October 18, 2024), https://www.maine.gov/cgi-bin/agviewerad/ret?loc=1394 (last visited November 14, 2024).
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

31. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive PII of Plaintiff and Class Members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

33. Defendant admits that an unauthorized third-party accessed its IT Network and obtained sensitive PII.

34. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

35. The PII that Defendant allowed to be exposed in the Data Breach is the type of PII that Defendant knew or should have known would be the target of cyberattacks.

36. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[18] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' PII.

37. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[19] Immediate notification of a data breach is critical so that those impacted can take measures to protect themselves.

38. Here, Defendant waited nearly a month after being made aware of the Data Breach to notify impacted individuals.

---

[18] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited November 14, 2024).

[19] *Id.*

D. The Harm Caused by the Data Breach Now and Going Forward

39. Victims of data breaches are susceptible to becoming victims of identity theft.

40. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[20]

41. The type of data that was accessed and compromised here – such as, Plaintiff's name and Social Security number – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access.

42. Plaintiff and Class members face a substantial risk of identity theft given that their Social Security numbers and other important PII was compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

43. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

44. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[21]

---

[20] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited November 14, 2024).

[21] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE, (December 28, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited November 14, 2024).

45. For example, in one recent case unsealed by the U.S. Department of Justice, an Illinois man led a group of criminals in marketing almost 50,000 stolen payment cards on dark web marketplaces, generating at least $1 million in cryptocurrency.[22]

46. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, someone can purchase a full range of documents that will allow identity theft, including $500 for a high-quality U.S. driver's license, $25 for a hacked social media account, $110 for credit card information, and $150 for banking account information.[23]

47. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

48. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to

[22] *Is Your Information for Sale on the Dark Web?,* NASDAQ (Feb. 26, 2024) https://verafin.com/2024/02/is-your-information-for-sale-on-the-dark-web/ (last visited November 14, 2024).
[23] *Revealed – how much is personal information worth on the dark web?,* INSURANCEBUSINESS (May 1, 2023) https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx (last visited November 14, 2024).
[24] *Id.*

credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[25]

49. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[26]

50. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[27] Defendant did not rapidly report to Plaintiff and Class Members that their PII had been stolen, instead waiting nearly a month to issue a notice of public disclosure.

51. As a result of the Data Breach, the PII of Plaintiff and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual

---

[25] *Experts advise compliance not same as security*, RELIAS MEDIA (May 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited November 14, 2024).

[26] *2019 Internet Crime Report Released*, FBI (February 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (last visited November 14, 2024).

[27] *Id.*

understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII.

52. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

53. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and Class Members' PII; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

54. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for

which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

55. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in October of 2024 (the "Class").

56. Specifically excluded from the Class is Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

57. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

58. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

59. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

60. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because, Plaintiff, like the unnamed Class, had their PII compromised as a result

of the Data Breach. Plaintiff is a member of the Class, and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

61. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

62. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

63. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Class Member's PII was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff and Class Members' PII;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure individuals' PII;

i. Whether Defendant was unjustly enriched;

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

64. Information concerning Defendant's policies is available from Defendant's records.

65. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

66. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

67. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 22 through 54 as though fully set forth herein.

68. Plaintiff brings this claim individually and on behalf of the Class Members.

69. Defendant knowingly collected, came into possession of, and maintained Plaintiff and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

70. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' PII.

71. Defendant had, and continues to have, a duty to timely disclose that Plaintiff and Class Members' PII within its possession was compromised and precisely the types of information that were compromised.

72. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected individuals' PII.

73. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

74. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

75. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' PII.

76. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

77. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' PII within Defendant's possession.

78. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class Members' PII.

79. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

80. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Members' PII. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the PII it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

81. Defendant's failure to comply with applicable laws and regulations constitutes negligence.

82. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

83. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' PII would result in injuries to Plaintiff and Class Members.

84. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' PII to be compromised.

85. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

86. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

87. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

88. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 22 through 54 as though fully set forth herein.

89. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff and Class members' PII. Various FTC publications and orders also form the basis of Defendant's duty.

90. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff and Class members' PII and not complying with industry standards.

91. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

92. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

93. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

94. As a result of Defendant's negligence *per se*, Plaintiff and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

95. Plaintiff incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 22 through 54 as though fully set forth herein.

96. Plaintiff and the Class provided and entrusted their PII to Defendant. Plaintiff and the Class provided their PII to Defendant as part of Defendant regular business practices.

97. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was secure.

98. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their PII. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff sand Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' PII; and (3) protect Plaintiff and Class Members' PII in compliance with federal and state laws and regulations and industry standards.

99. Implied in these exchanges was a promise by Defendant to ensure the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' PII.

100. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' PII to be accessed in the Data Breach.

101. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

102. These exchanges constituted an agreement and meeting of the minds between the parties.

103. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' PII if it did not intend to provide Plaintiff and Class Members with its services.

104. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

105. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

106. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII.

107. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class Members violated the purpose of the agreement between the parties.

108. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

109. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 16 and paragraphs 22 through 54 as though fully set forth herein.

110. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their valuable PII.

111. Defendant appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Defendant also benefited from the receipt of Plaintiff and Class Members' PII.

112. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendant had they known Defendant would not adequately protect their PII.

113. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representatives of the Class and her counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 18, 2024

Respectfully submitted,

By: /s/ *Gary M. Klinger*

Gary M. Klinger (IL Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Eduard Korsinsky*
Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: ek@zlk.com
Email: msvensson@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiff and the Proposed Class